



Le fossé entre la  
gestion d'identités  
et les systèmes  
non-fédérés





## MAURICE CÔTÉ

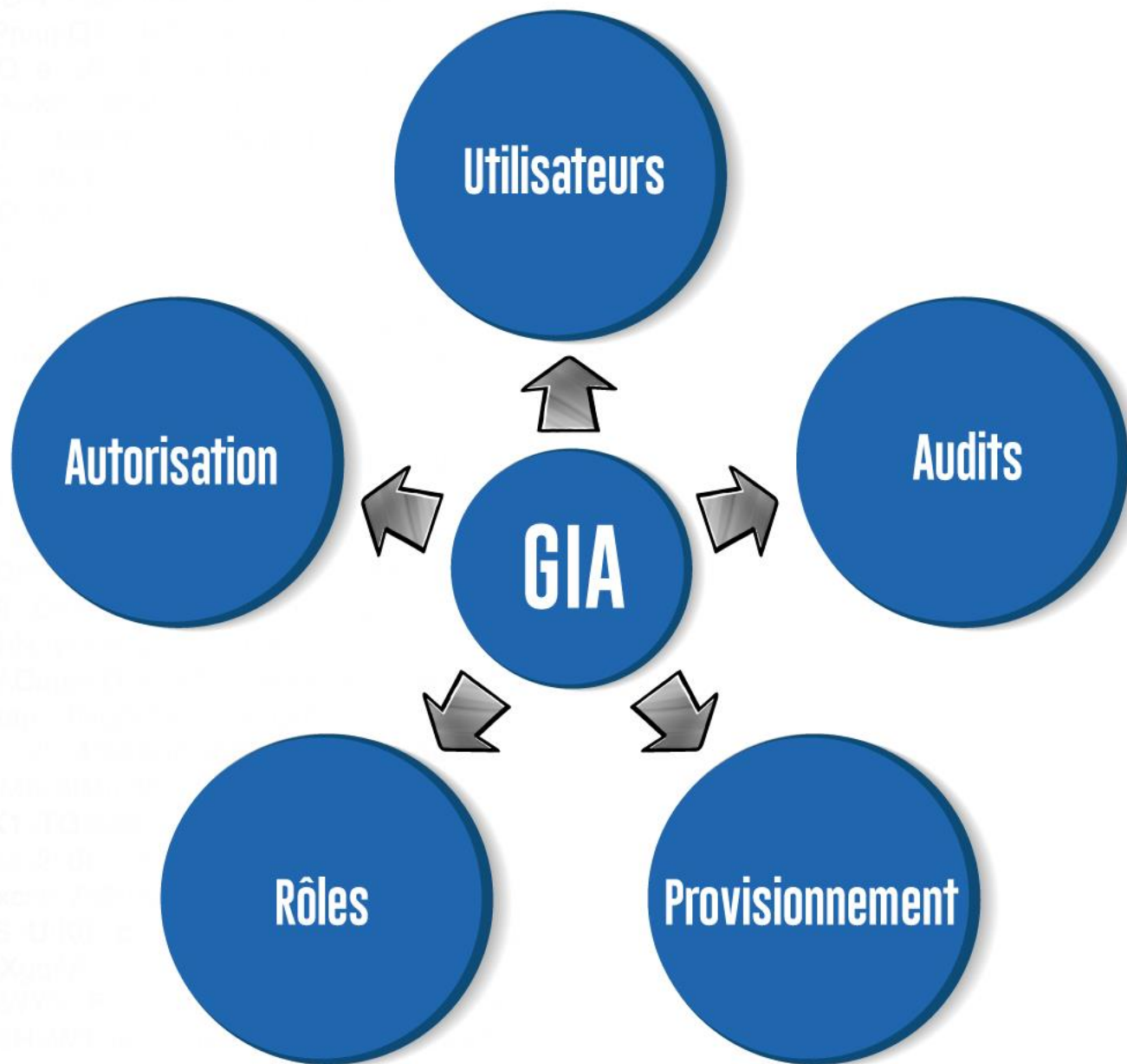
- Architecte d'affaires chez Devolutions depuis 2012
- Responsable du produit (PO) de gestion d'accès privilégiés (PAM)
- Collabore avec des analystes et des partenaires PAM
- Fortement impliqué dans les programmes de conformité (SOC2, RGPD, etc.)

# Gestion d'identités

La gestion des identités et des accès (GIA) (ou IAM pour Identity and Access Management) est un cadre de processus, de politiques et de technologies qui facilitent la gestion d'identités électroniques et numériques.



# Gestion d'identités



# Gestion d'identités

- L'industrie tend vers l'utilisation d'un fournisseur d'identité (IdP) unique pour tous les systèmes de l'entreprise.
- Même que certaines personnes rêvent que les produits ne soient plus associés à un seul fournisseur, mais plutôt qu'une personne puisse choisir quel fournisseur confirmera son identité afin que cette personne n'ait qu'une seule identité numérique!
- Dans ce cas, le système IAM doit quand même gérer les groupes d'utilisateurs, les rôles, etc.

# En quoi y a-t-il un fossé?

Malheureusement, certains équipements ou applications ne permettent pas d'utiliser d'autres fournisseurs d'identité :

- anciens systèmes
- systèmes personnalisés
- systèmes internes

Effectivement, les IdP modernes comme AzureAD (Office365), Okta et Auth0, sont conçus pour être compatibles avec un plus grand nombre de produits. Leur intégration est également facile, alors le fossé sera partiellement comblé, mais engendrera tout de même des coûts d'intégration.

# Les systèmes non-fédérés

## Matériel informatique

- Équipement reseau
- Imprimantes
- Machines spécialisées

## Comptes partagés

- Applications d'entreprise d'ancienne generation
- Comptes de réseaux sociaux
- Comptes pour des tâches spécifiques

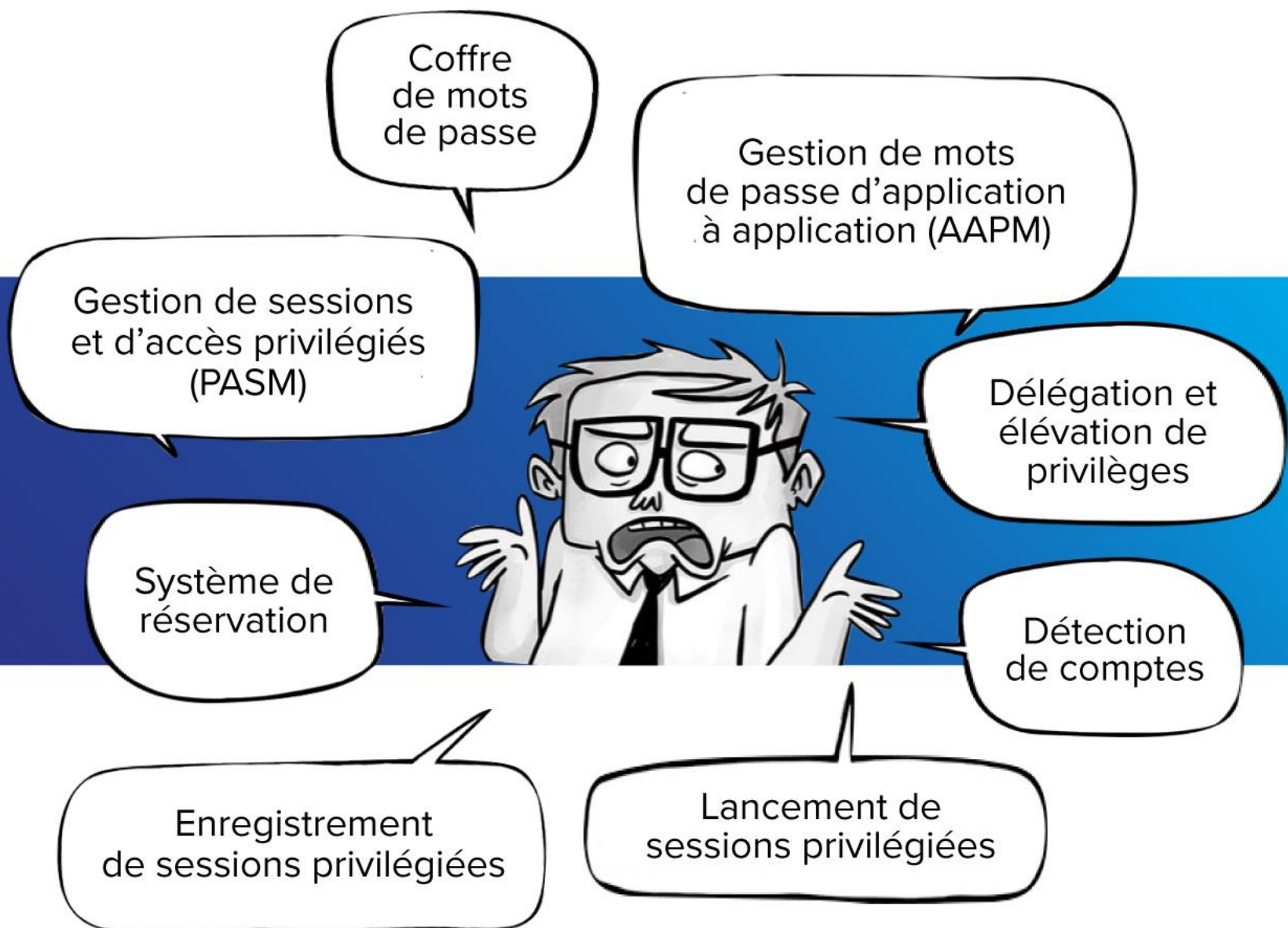


# Qu'est-ce que la gestion d'accès privilégiés (PAM)?





# Qu'est-ce que la gestion d'accès privilégiés (PAM)?



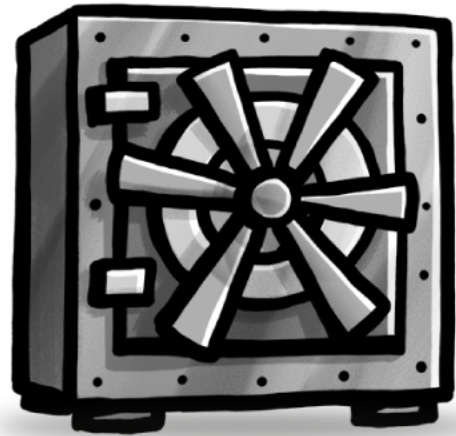
# Comptes privilégiés



- Comptes administrateur de domaine
- Comptes d'utilisateurs privilégiés
- Comptes administrateur locaux
- Comptes d'accès d'urgence
- Comptes système
- Comptes de services (domaine)

# MODULES PAM

## COFFRE



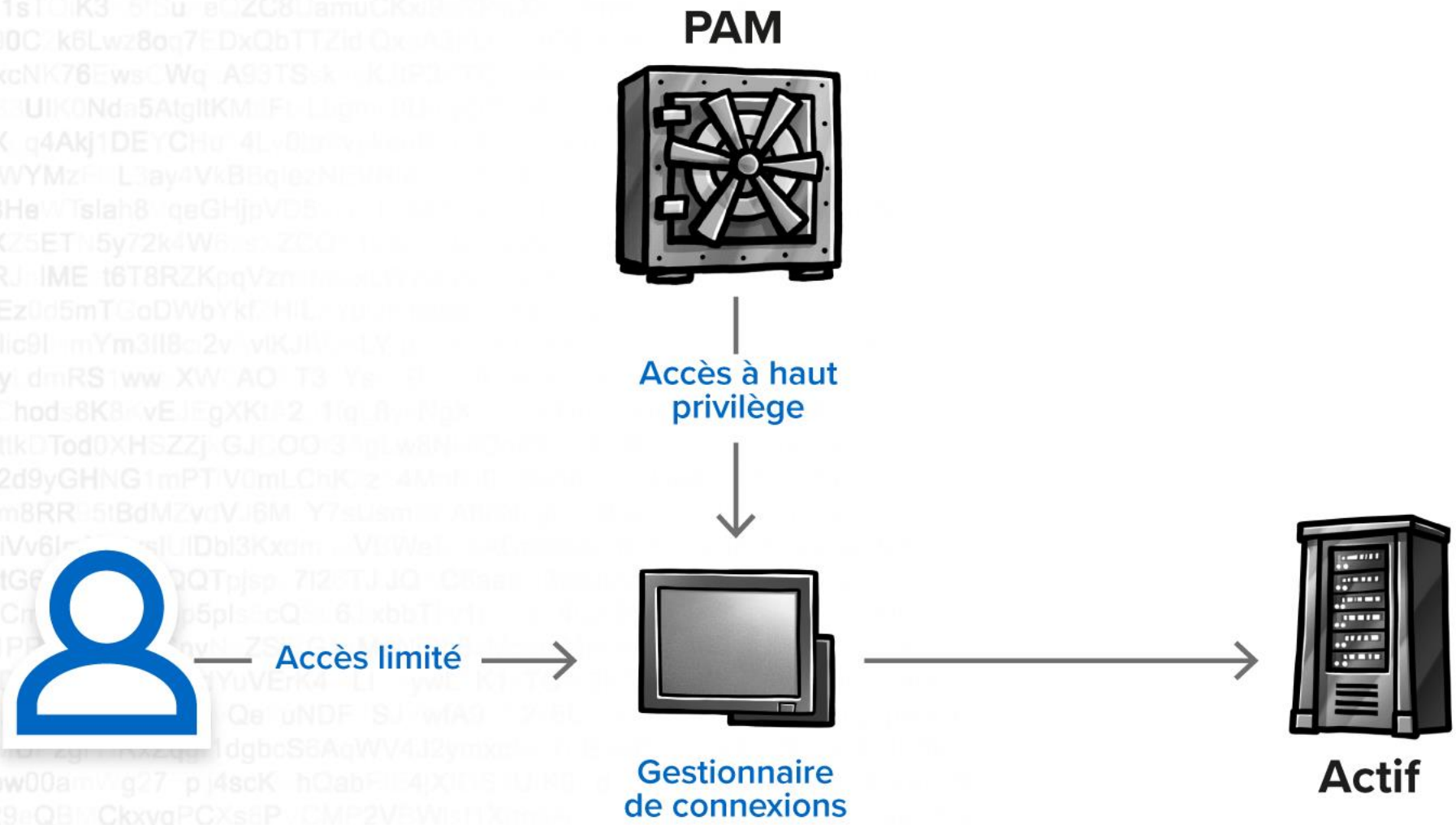
- Stockage sécurisé de comptes privilégiés
- Accès restreint aux comptes privilégiés
- Détection de comptes
- Rotation de mots de passe
- Scénarios en cas d'urgence / Break the glass



# MODULES GESTION DES ACCÈS PRIVILÉGIÉS **GESTION DE SESSIONS**

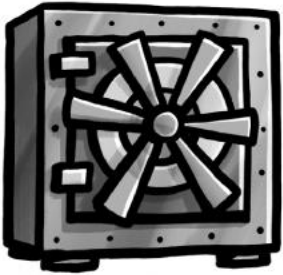


- Lancement de sessions
- Authentification des utilisateurs
- Autorisation
- Authentification unique pour se connecter aux systèmes ciblés
- Surveillance et pistes d'audit des activités dans les comptes privilégiés



UIDb13 x1mguVBWeE8cACAop8DsKkVUoZ R9 6Vs9 J KN...  
bQQTpj pL7126TJJQAC 6a pU3txgIM7s 6 SeQrOKKkC4 bEJON...  
jdp5pls5cQ 1L6JjxbTfy1tQVb 4QABp08Z497Vul0P2...  
SnvNdZSj G1xMaNiBh8x bzoiMm3Ma 3c5rX 8RCgb yJZ...  
HldYuVERk mLINvywLT 1sTCK3 5Su eCZC8UamuCKx9...  
m5qvQe8uNDFZSJvwfA90C k6Lwz8oq7EDxQbTTZid Qx...  
g r1dgbcs6 qWV4J2ymxcNK76EwsC Wq A93TSak K10...  
Ep 4scKwhQ b IE jXIO UIKONd 5AglIKM FiLdg...  
CXs8PVCMP 2VBWIs1X q4Akj1DEYCh 4L00mV...  
6Hj ByVhhznnGGERTaOWYmzF L3ay4VkB8qiazN5VR...  
JeCeJch1cfmYxfvI7HsBHe VtSlah8 qaGHjpVD5...  
eZz7XpqcX5rdg pInUNXZ5ETm5y72k4W0...  
bAJ9RLBFdV0VuOizprMRJ IME t6T8RZKpqVzn...  
ESK8vi3198HmO38aEz0d5mTGoDWbYkf HIL...  
aKq22otjCaNV8WIQBNj7lic9l mYm3ll8c2v viKJIV...  
CzPM wbZy0xyumbcivRy dmRS ww XW AO T3 Ys...  
pZih 5dNOxGzKmRHo8 Chods8K8 kvE JEgXKI2 1q...  
FvZ1hoW AzGpV5... KKTod0XHSZzj GJC00 3...  
bLQnZHWt bVE... 9yGHNG1mPT V0mLChK z 4M...  
9DooOsV21uMh... RR 5tBdMZvV i6M Y7sUsm...  
AQxP5zMjSO12... 6ImYv x...  
xd9NcQGgN...  
Rls7 Cqd8z... hmZr1jdp5pls cQ 1L6J xbbT...  
cf sUkWgzx... GjmSnvV ZSj G1 MaNiBh8...  
nd9ZzpW3o zonJ5ad6aDk7i4qiSi0B HldYuVERk4...  
vIXHutePLS v5kqipWN xZNKZl qsb0 m5q Qe uNDF...  
3HWok0gb0sH73OPcyZMUPzgr lRxZqgr1dgbcs6AqWV4J2ymxc...  
gve aCt gfi9Adp6FjCbjbw00a... g27 p j4scK nQabF...  
29jW15 WwNIURZZ7 Y29eQ8 CkxygPCxs8P CMP2V...  
Sy 7cQ A6IC9snNQvzbWXmdQ LaEv6HjcByVhh...  
EByy FMHU PsgBfFuj p7esjPRKLP2nUeC... 1cfmYxfvI7...  
y:qtJMs bjmTDGGQswaK JKZ0 r3l eZz7XpqcX5r gwpIn...  
22c0tNxxqgyANEyQJ0vJgSj XPQ gmdbAJ9R BFdV VuQ...  
bf7c0LAyeQeCFSeGa4pM6I9EIXVivG11y1ESK8v 3 198H...  
Q23kDmsACo0tBc q7wmvB5EHLkFRakQ22otCaN...

**PAM**



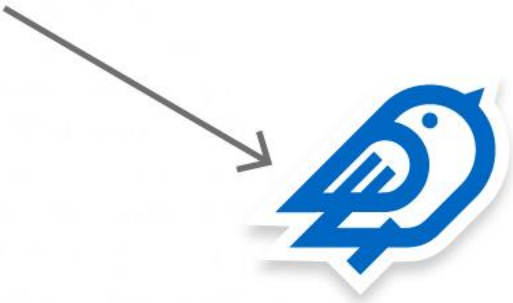
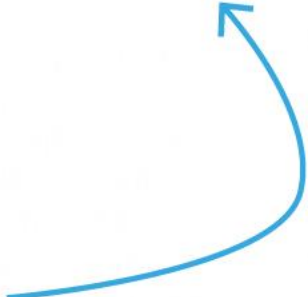
Accès à haut privilège



Gestionnaire de connexions



Accès limité



Sessions privilégiées (Passerelle / Bastion)

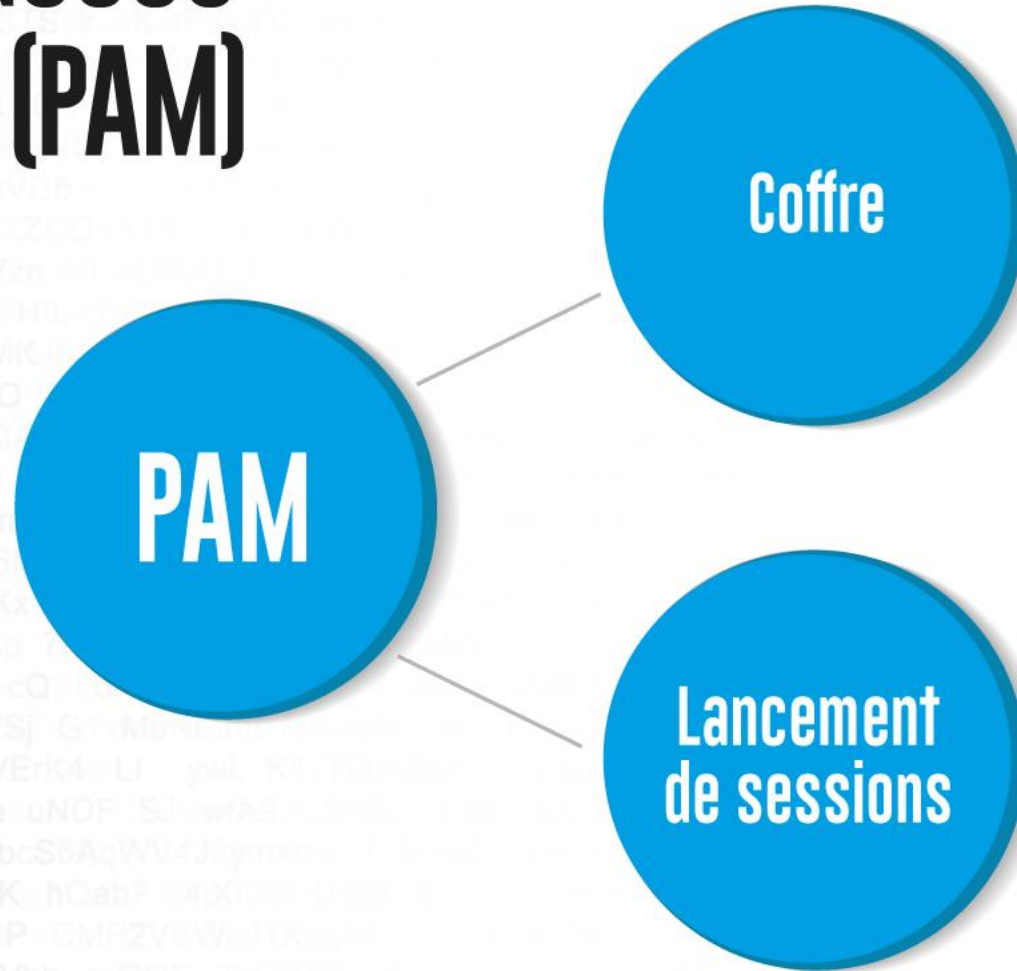


Actif



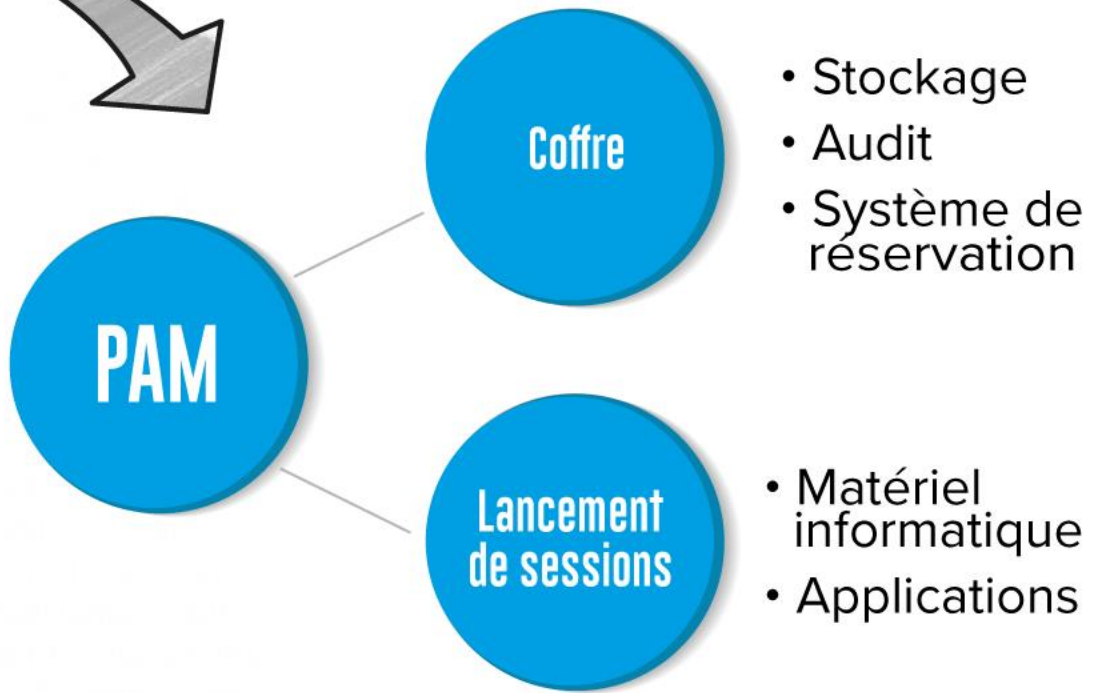
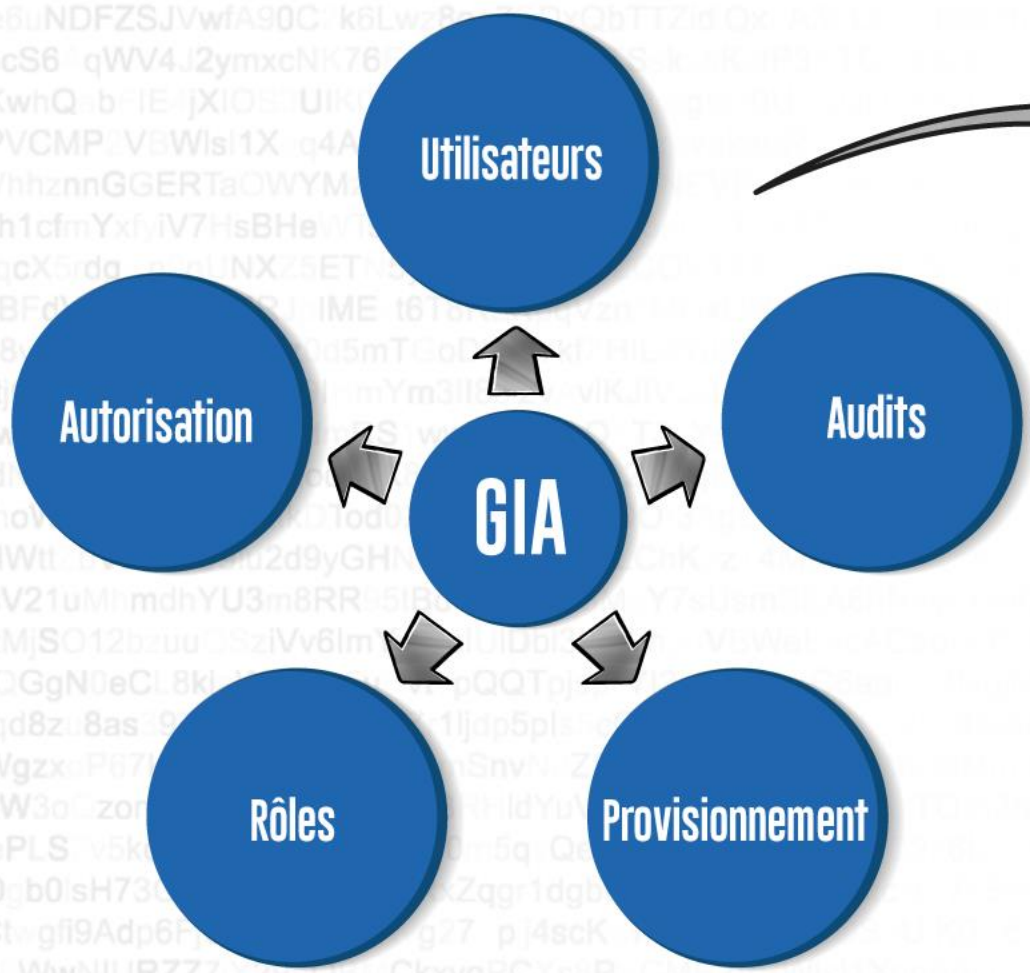
# Gestion d'accès privilégiés (PAM)

## La base



- Stockage
- Audit
- Système de réservation

- Matériel informatique
- Applications



- Stockage
- Audit
- Système de réservation

- Matériel informatique
- Applications

# Comblé le fossé

- La solution PAM se sert des identités gérées par votre solution IAM pour attribuer une identité unique aux utilisateurs et leurs rôles.
- Le contrôle d'accès basé sur les rôles du PAM octroie des permissions aux utilisateurs en fonction de leur rôle auxquels ils sont associés.
- Les événements et les alertes, en plus d'une intégration de Syslog, peuvent compléter les journaux de la solution IAM et aident à surveiller les activités des utilisateurs.



# Offrir des solutions alliant productivité et sécurité aux professionnels des TI.



Pour plus d'informations, visitez notre site Web au  
<https://devolutions.net/fr>

